isi UPDATE

ISSUE 1 | NOVEMBER 2007

NEWSLETTER OF THE INFORMATION SECURITY INSTITUTE

from the directors

Mr Eric Hall, General Manager and Director of Business Development

Professor Ed Dawson, Research Director

Over the last 12 months there has been an increasing move by government and private industry in Australia to move to an electronic environment. This includes areas critical to the existence of a modern society such as health records and control of water and electricity supply. At the same time cyber attacks have become more sophisticated and common with international organised crime playing a significant role in such attacks. Identity theft and botnet attacks are problems that are facing individuals and corporate networks on a worldwide basis. These developments highlight the importance of research into information security.

Over the last 12 months researchers from the ISI have been actively involved in many different areas of research to assist government and private organisations. This includes developing tools to identify financial fraud, developing security systems for health records, designing security and legal frameworks for federated databases for e-government, designing tools for computer forensics, strengthening security mechanisms for SCADA control systems for water and electricity, designing security and legal frameworks for e-business in the construction industry, developing intrusion detection tools for both wired and wireless networks, designing video surveillance tools, designing speaker verification and recognition techniques, and designing more secure and efficient cryptographic protocols and algorithms. As part of this research effort, the ISI has been involved in collaborative partnerships with many different organisations including Construction Innovation CRC, Smart Internet CRC, AutoCRC, NICTA, CSIRO, DSTO, Brisbane Airport Corporation, Motorola, Australian and Queensland Government Departments.

In co-operation with the ARC network Research Network for a Secure Australia (RNSA), the ISI has hosted several national and international conferences. These include the 12th Australasian Conference on Information Security and Privacy (ACISP) in Townsville, the 10th Recent Advancements in Intrusion Detection (RAID) conference at the Gold Coast and the 3rd Indo-Australian IT Security Conference (IACITS). It should be noted that this was the first time that the RAID conference, which is the leading international conference on intrusion detection was held outside of North America and Europe.

in this issue

new funded projects

- **Department of Prime Minister and Cabinet – National Security Science and Technology Unit (NSSTU), Research Support For Counter-Terrorism**

  1. Dr Andrew Clark [FIT] *'Incident Response in Control Systems Environments'* 1 year project, the total cash funding is $100 000 from NSST and DSD

- **ARC Discovery**

  1. Professor Ed Dawson [ISI], Professor Stephen Corones [LAW], Professor Bill Lane [LAW], Dr Ernest Foo [FIT], Dr Adrian McCullagh [ISI], *'Technical and Legal Models for Virtual Info-Sharing Networks (VISN) for Critical Infrastructure Protection (CIP)'*, Total Funding Approved: $382 000 for 3 years.

  2. Professoor Colin Boyd [FIT], *'Cryptographic Protocol: Proofs and Designs'*, Total Funding Approved: $222 000 for 3 years.

- **National Institute of Information and Communication Technology (NICT)**

  1. Professor Ed Dawson [ISI], Professor Colin Boyd [ISI], Professor Javier Lopez (University of Malaga, Spain) and Professor Eiji Okomoto (Tsukuba University, Japan), *'Privacy – NICT'*, On-going collaborative project, Total Funding: $150 000.

- **ARC Linkages – 2007 Round 2**

  1. A/Professor Audun Josang [FIT] – Total Funding Approved: $228 000 (ARC) and $81 420 (SAP) for 3 years

  2. Professor Colin Fidge [FIT] – Total Funding Approved: $120 000 (ARC) $75 000 (DSD) for 4 years

  3. Professor Colin Boyd [FIT] – Total Funding Approved: $256 000 (ARC) $90 000 (Motorola) for 4 years

QUT isi Information Security Institute

isi diary

CONFERENCES

The ISI hosted the following conferences and workshops this year:

- The 3rd Indo–Australian IT Security Conference (IACITS 2007) held at QUT, 9–10 July, 2007 [57 attendees].
- The 12th Australasian Conference on Information Security and Privacy (ACISP 2007), held in Townsville, 2–4 July, 2007 [55 attendees]
- The 10th International Symposium in Recent Advances in Intrusion Detection (RAID 2007), held on the Gold Coast, 5–7 September, 2007 [80 attendees]
- ICE-EM RNSA Pairing Based Cryptography 2007 Workshop comprising a 3 day Lecture Series followed by a 2 days Workshop, held at QUT, 25–29 June, 2007 [28 Lecture Series attendees and 43 Workshop attendees].
- RNSA 'Network Monitoring' Workshop held on the Gold Coast, 4 September, 2007 [35 attendees].

VISITORS TO ISI

- Professor Raghavan (ITT, Madras)
- Dr Andreas Enge (Ecole Polytechnique, France)
- Dr Kenny Paterson (Royal Holloway, University of London)
- Professor Rama Chellapa (University of Maryland, USA)

ISI KEYNOTE TALKS AT INTERNATIONAL CONFERENCES

Boyd, C., (Invited Speaker) 'One Pass Key Establishment' **ProvSec 2007**, held in Wollongong, Australia, 1–2 November, 2007

Caelli, W.J., (Keynote Address) 'Application Security–Myth or Reality' **ISPEC 2007**, held in Hong Kong, 7–9 May, 2007.

Caelli, W.J., (Keynote address) 'Modernising MAC: New Forms for Mandatory Access Control in an Era of DRM' **IFIP/Sec 2007** held in Sandton, South Africa. 14–16 May, 2007.

Dawson, E., (Keynote Address) 'Electronic Government Commercialisation of Information in a Federated System' **Information Security Summit**, held in Prague, Czech Republic, 17–18 May, 2007.

privacy protection: QUT leading the way in e-security and privacy

Professor Peter Croll

NEW IT security measures have been developed by QUT that minimise the threats posed by unauthorised access or snooping into people's private health records. Researchers from QUT's Information Security Institute have been collaborating on two separate projects, both aimed at protecting private information from the eyes of the public.

IT privacy expert Professor Peter Croll and IT security expert Professor Bill Caelli said the privacy threat from company 'insiders' was very real with unauthorised access to sensitive data often readily obtained. 'At QUT we have developed the first software demonstrator suitable for data protection in the health care sector and in fact all businesses, that makes it highly improbable for information to be accessed without authorisation,' Professor Croll said. 'If an enterprise has a security policy then this software can enforce that security policy so that it can't be overridden. 'It offers military-level, mandatory access controls to ensure privacy is enforced in commercially available, enterprise-level computer systems.'

Professor Croll said the development of this prototype, funded by the Australian Research Council, provided strict access control technology to prevent unauthorised viewing of sensitive data.'The privacy of health care records is a fundamental concern because any exposure is simply irreversible,' he said. 'It is a further concern that in many cases sensitive medical information may not be known to a person's partner or family members. 'In particular, typical home computers shared by family and household members are simply not suitable in any way for the storage and display of such data.'

Professor Croll said while the software was primarily developed to protect health data, it could be applied to all commercial businesses and organisations.

Professor Caelli said QUT, in collaboration with the CSIRO's E-Health Research Centre, had also developed another security measure to protect people's privacy. 'This is a web-based software tool that asks questions of the user and then makes sure that the user is aware of the relevant privacy regulations and rules before allowing access to information,' he said. 'It encourages privacy policy compliance and provides applications with enhanced access control parameters. 'Combined with strict access control software, these tools could provide tough security to protect private information.' Professor Caelli said QUT was leading the way in e-security and privacy and postgraduate students were working with a number of key authorities to further undertake research in this area.

Project	Research Team	Funding	Partners	Contact
Develop the tools and techniques to protect e-health records	Professor Peter Croll Professor Bill Caelli Dr Matt Henricksen	QUT CSIRO Australian Research Council	QUT Information Security Institute CSIRO E–Health Research Centre	Prof Peter Croll +61 7 3138 1956 p.croll@qut.edu.au

Solutions Published by QUT's Marketing and Communication Department in cooperation with QUT's Research and Commercialistion Division, QUT Publications 1429, p.20

case study: information security policy

Professor
Bill Caelli

Finding better ways to safeguard information is not merely a matter of research to develop new technologies and systems. The three areas identified by QUT's Information Security Institute (ISI) –technology, policy, governance–reflect the central place of disseminating information and influencing government policy and institutional governance in achieving and sustaining information security. A further need is to educate the public, from company directors to schoolchildren, about the importance of information security issues.

Professor Bill Caelli AO, the leader of the policy area in the ISI, has made a unique contribution to establishing information security in the academy as well as to leading public debate in the area through policy formation, information dissemination and media commentary. He stresses that academic debate about information security, and indeed the whole discipline of information and telecommunications technology, are often responses to industry developments–both within the computer industry itself and in the increasingly sophisticated applications of information technology across virtually every sector of the economy, public and private. 'Market pull', as he puts it, can determine 'technology push' and shape the contribution that academic information technology departments can make.

Caelli's own working life is an interesting study in both the development of the IT industry and its gradual incorporation into universities. He entered university well before the advent of tertiary IT courses, and trained initially as a physicist. But he soon found himself part of the fledgling computer industry, writing his first computer program in 1959 while in high school and later working for a number of IT companies in Australia and with them in the US. Caelli started his own company, Eracom Pty Ltd, in the late 1970s, initially focusing on building advanced desktop workstations, with inbuilt security features unique at the time. By the mid–1980s the company had moved fully into the emerging information security field, as new commercial technologies such as EFTPOS created a huge market for secure information systems involving cryptographic components.

It was initially a shortage of graduates with skills in information security that prompted Eracom to approach the then Queensland Institute of Technology in 1988. The result was the QIT Information Security Research Centre, funded through an agreement with Eracom. The Centre, one of the first in the world devoted to the field, conducted industry training and academic courses as well as research, with modules eventually configured into a graduate certificate program. After some years dividing his time between Eracom and QUT, Caelli eventually became a full–time academic, taking up the post of Head of the new School of Data Communications in the Faculty of Information Technology in 1994.

Bill Caelli says that he never saw information security as purely a technical or scientific matter. From an early stage, he was committed to involving other areas of QUT, from law and business to sociology, that could contribute to an understanding of the complex social, commercial and technical aspects of the field. The ISI reflects this approach today, with the involvement of the Faculties of Law and of Business, as well as Information Technology.

As one of the early movers in developing information security as an academic field in response to industry and social needs, Caelli has been well placed to be a leader in shaping public debate in the field. He serves on two advisory committees within the Australian Government's Trusted Information Sharing Network, one specifically concerned with information technology security issues and one with considering more general and longer term threats to the infrastructure of the nation. These groups commission research and technical reports, which are the basis of policy advice to governments or 'best practice' documents for industry. Caelli has also developed a career as a media commentator on privacy, internet banking and allied topics.

Caelli has also made an international contribution to shaping public debate about the field as the only non–American on a peak organisation for information security education, the Colloquium for Information Systems Security Information (CISSE). He is also a long serving member of the security and privacy technical committee of the International Federation for Information Processing (IFIP), the peak organisation of national computer societies that brings academic and industry groups together on a global basis. He was made in Officer in the Order of Australia for these services in 2003.

Challenging Boundaries Perspectives on Community-University Engagement, 2007 QUT Publications 13479, pp, 60-61

robust speaker recognition with reduced utterance duration and intersession variability

Professor Sridha Sridharan

Technological advances pioneered by the Speech and Audio Research Lab in the area of Automatic Speaker Verification (ASV) have lead to a successful application to the highly regarded and competitive Australian Research Council (ARC) Discovery Grant programme.

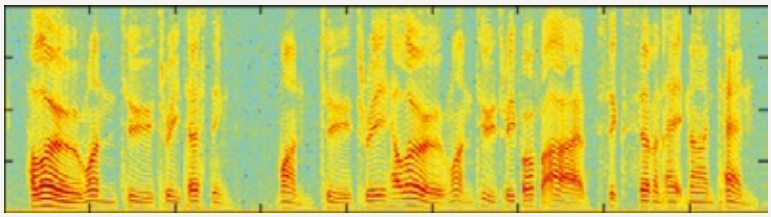
Speaker verification is the process of verifying a person's identity by analysing their speech, or through their 'voice print'. There are several important security applications for ASV technology including suspect identification, terrorist tracking and detecting a person's presence at a remote location, as well as person authentication for phone banking and credit card transactions.

Telephones and telephony networks are a natural match for these applications but introduce several difficulties. Specifically, background noise, telephone handset differences, network distortions and room acoustics are common sources of errors for ASV systems.

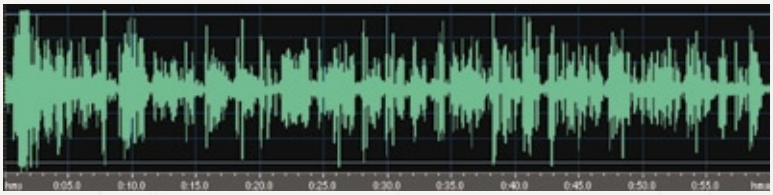
The advances introduced by research at the Speech and Audio Research Lab have halved the error rates of telephone-based ASV. This was achieved by developing a model that directly incorporates the environmental conditions of a recording as an observable variable which allows the true characteristics of the speaker to be measured more accurately. This advance, known as Explicit Session Variability Modelling, has seen QUT at the forefront of this research field as demonstrated in world-wide performance benchmarking.

Explicit Session Variability Modelling has since been adopted by the leading research centres in speaker verification throughout the world and is currently a hot topic of research.

Professor Sridha Sridharan has recently received approval from the ARC for a grant under the Discovery Project program to support continued research into session variability modelling. This grant, worth almost $200 000 over three years, will support research that is conservatively estimated to again halve ASV error rates through extending the session variability modelling and building on recent advances in the field of statistical pattern recognition.



High energy frequency and resonance patterns of speech can be used to identify people on the shape of their vocal tract



Advanced signal processing and pattern recognition algorithms are used to transform a speech waveform into a unique statistical model of a speaker

Project Leader Professor Sridha Sridharan [BEE]
Researchers Prof S Sridharan and Dr R Vogt

achievements

Outstanding ISI researchers and their contribution to QUT and/or the wider community

- The Dragon Encryption Algorithm designed by ISI team led by Prof Ed Dawson has been selected as a phase three finalist for profile 1 (Software) for 'eSTREAM' in the ECRYPT Steam Cipher Project, ref: www.ecrypt.eu.org/stream/

Professor Bill Caelli, AO

- 'Fellow of (ISC)2'. On 26 April, 2007 William J Caelli, became the world's first recipient of a fellowship with (ISC)2 the globally recognised certifying body for information security professionals. This is a Certification established to recognize select information security professionals who have made outstanding lifetime contributions in the field.
- On Tuesday 5 June 2007 at the 11th conference of the Colloquium for Information Systems Security Education (CISSE) (URL:www.cisseinfo) hosted by Boston University in Boston, Massachusetts, the 2007 'William Hugh Murray Founders' Award' was presented to three recipients. Professor William J (Bill) Caelli, AO was honoured as one of those recipients at the ceremony.

Dr Robbie Vogt

- Participated in National Institute of Standards and Technology (US) evaluation of his speaker recognition technology and finished in the top three.

Dr Andrew Clark and Dr Clinton Fookes

- Nominated for the 2007 Vice–Chancellor's Award for Excellence

Dr Jason Reid and Dr Jason Smith

- Recipients of the 2007 Vice-Chancellor's Performance Awards

new appointments

- Terry Stevenson – Adjunct Professor (BEE)
- Robbie Vogt – Researcher (BEE)
- Paul Barnes – Deputy Director (BUS)
- Bill Caelli – Emeritus Professor (FIT)

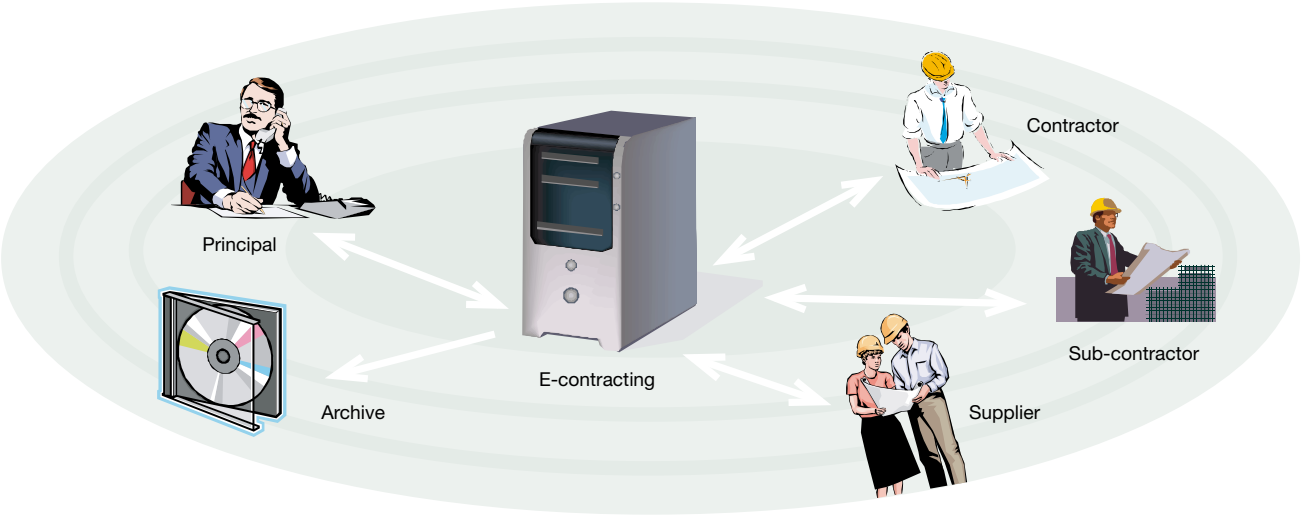
electronic contract administration – legal and security issues

Professor Sharon Christensen

Electronic contract administartion – Legal and security issues, is a collaborative research project funded by the Cooperative Research Centre for Construction Innovation. This multidisciplinary research project is supported by six project partners and seeks to assist the construction industry in transporting its contracting processes into an electronic environment.

The objectives of this research project are to identify the legal and security risks that arise when construction contracts are formed, administered and recorded within an electronic environment and to provide industry participants with practical recommendations to minimise these risks. These objectives have been achieved through the production of a Final Research Report containing detailed recommendations for secure and legally compliant electronic contracting.

Participants in the construction industry will also benefit from a range of other research materials produced by this project. Legal and information technology professionals will benefit from an extensive literature review that has been produced, containing a detailed analysis of national and international literature, legislation and case law on electronic contracting. Information technology professionals may also benefit from a Scoping Study and examines a number of online collaboration platforms currently used by the construction industry and identifies the required security features for a collaboration platform to facilitate effective electronic contracting.



Project Leaders Sharon Christensen (LAW) **Team Members** Martin Betts, Debbie Smith (BEE), Bill Duncan, Kathryn O'Shea (LAW), Ed Dawson, Ernest Foo, Audun Josang (ISI) **Researchers** Judith McNamara (LAW), Praveen Gauravaram (FIT)

visiting postdoctoral fellow

Havard Raddum

My name is Havard Raddum, and I come from the University of Bergen, Norway. I finished my Ph.D. in February 2005, and got a position as a postdoc right afterwards. A few months later I applied for my own postdoc project with the Norwegian Research Council, doing research on the non-linear equation systems that arise in cryptanalysis. Since the research council likes international cooperation and strongly encourages visits abroad, I looked for possible places to go when preparing the application. Our group in Bergen had previously had a student at the ISI for a year and I had only heard nice things about Brisbane, so that was on the top of the list of where my family and I would like to go. It was not hard to get a letter of invitation from Ed Dawson and with that in the application I was lucky enough to get the grant, including money to cover the extra expenses for relocating to Brisbane.

We arrived in January this year, and it didn't take long to find a house and get a normal everyday routine up and running for the whole family. Brisbane has not been a disappointment and I can very well understand why people choose to settle down here, making it the fastest growing city of Australia. I have also been very well received at the ISI. When my family and I head back to Norway in December it will be with lots of good memories from our time here.

For those of you lucky enough to get the opportunity for a stay overseas visiting a different country, I can only encourage it. More often you regret the things you didn't do than the things you do.

isi tackles fraud

Dr Andrew Clark

QUT has joined forces with international enterprise software giant SAP to combat Australia's worsening $3 billion financial fraud problem. A research team from the Information Security Institute (ISI) at QUT has embarked on a three-year project investigating approaches for automating the detection of fraud within organisations. The project has the support of the Australian Research Council through its Linkage Projects scheme.

ISI researcher Andrew Clark said that, according to a recent survey by KPMG, financial fraud committed by internal sources accounted for 54 per cent of fraudulent activity in the non-financial services sectors.

"Aside from outright theft, most fraud occurs through misappropriating funds, forged cheques, falsifying invoices and computer fraud," Dr Clark said. He said SAP had put considerable effort into fraud prevention and was now eager to explore how they could enhance their systems to include an automated ability to detect fraud. In Australia, SAP enterprise applications are employed by many hundreds of midsized businesses as well as some of the largest organisations in the country. "The idea is to monitor invoicing and salary payments, for example, and to try and identify unusual instances of those that may be indicative of fraudulent behaviour by personnel within the organisation," he said. "For example, someone who works in invoicing might change the bank account details of a supplier so that an invoice is paid into their personal bank account, and then change the number back to avoid detection. "At the moment, that kind of transaction may only be picked up by accountants or auditors working manually through records."

Dr Clark said the project's goal was to develop algorithms and methods of aggregating different types of event data about the activities that people in organisations perform on computer systems. "These can then be applied to a system that helps us identify anomalous behaviour and produces an alert which would then have to be manually investigated by the appropriate person." Dr Clark said it was important, in fraud detection, to apply more generic techniques rather than trying to prescribe the types of behaviour that might be equal to fraud.

"It is a cat and mouse game because once fraudsters know you're looking for particular behaviour, they will change their behaviour in order to avoid detection. "The SAP system will look for unusual activities, and that will give us a broader coverage.".

Project	Research Team	Funding	Partners	Contact
Automatic detection of fraudulent activity	Adjunct Professor George Mohay (QUT) Dr Andrew Clark (QUT) Dr Julien Vayssiere (SAP) Associate Professor Peter Best (University of Southern Queensland)	$255 000 Australian Research Council Linkage Grant	QUT Information Security Institute SAP	Contact Dr Andrew Clark +61 7 3138 9550 a.clark@qutedu.au

Inside QUT September 18 – October 15, 2007 p.4. Story by Carmen Myler, and **Solutions** Published by QUT's Marketing and Communication Department in cooperation with QUT's Research and Commercialistion Division, QUT Publications 14292, p. 21

completions

Masters

- Dr Michael McGreevy – Dr Michael Mason (Associate) (BEE), ***Statistical Language Modelling for Large Vocabulary Speech Recognition.*** Supervisors: Professor Sridha Sridharan (Principal), Dr Michael Mason (Associate)
- Tim Lane (FIT), ***Information Security Management in Australian Universities – An Exploratory Analysis.*** Supervisors: Dr Lauren May (Principal), Dr Neville Thomas Meyers and Dr Kavoos Mohannak (Associates)

PhD

- Christopher McCool (BEE), ***Hybrid 2D and 3D Face Verification.*** Supervisors: Associate Professor Vinod Chandran (Principal), Professor Sridha Sridharan (Associate)
- Andrew Strange (BEE), ***Robust Thin Layer Coal Thickness Estimation Using Ground Penetrating Radar.*** Supervisors: Associate Professor Vinod Chandran (Principal), Professor Sridha Sridharan (Associate), Dr Jonathon Ralston (Industry Supervisor)
- Jaimee Brown (FIT), ***Secure Public-Key Encryption from Factorisation-Related Problems.*** Supervisors: Dr Juanma Gonzalez Nieto (Principal), Professor Colin Boyd, Professor Edward Dawson(Associates), Dr Paul Montague (Industry Supervisor)
- Praveen Gauravaram (FIT), ***Cryptographic Hash Functions: Cryptanalysis, Design and Applications.*** Supervisors: Dr William Millan (Principal), Dr Lauren May (Associate)
- Jason Reid (FIT), ***Enhancing Security in Distributed Systems with Trusted Computing Hardware.*** Supervisors: Professor Edward Dawson (Principal), Professor William Caelli, Professor Mark Looi (Associates)
- Jason Smith (FIT), ***Denial of Service: Prevention, Modelling and Detection.*** Supervisors: Dr Selwyn Russell (Principal) , Dr Juanma Gonzalez Nieto, Professor Mark Looi (Associates)
- Chaw (Charles) Woo (FIT), ***Digital Image Watermarking Methods for Copyright Protection and Authentication.*** Supervisors: Dr Jiang Du (Principal), Professor Binh Pham (Associate)

QUT isi Information Security Institute

Please contact us
CRICOS No. 00213J

Information Security Institute
Queensland University of Technology
GPO Box 2434 (126 Margaret Street)
Brisbane Qld 4001 Australia

Phone +61 3 3138 9572
Fax +61 7 3221 2384
Email info@isi.qut.edu.au
Web www.isi.qut.edu.au